TMA

Uniform Business Office

HIPAA Refresher for UBO Staff

Presented by the

UBO Program Support Team

Call in number: 1-866-866-2244

Participant Code: 5260345#

NOTICE

- This interactive telephone conference is intended for Uniform Business Office staff.
  - It does *not* replace the annual Information Assurance training requirement.
- HIPAA Training is provided through the MHS Learn system.
  - https://mhslearn.satx.disa.mil/ilearn/en/learner/jsp/default.htm
- For more information on MHS Learn, visit the TMA Privacy Office website.
  - http://www.tricare.mil/tmaprivacy/hipaa/hipaacompliance/tools-training/MHSLearn.htm
- If you have not already completed your HIPAA training, please do so as soon as possible.

Teleconference Goals

- Review those parts of the Health Insurance Portability and Accountability Act that apply to UBO staff
  - Privacy
    - A brief history, what is PHI, what can the billing office disclose
  - Security
    - How can a security breach occur
    - How to avoid a breach
  - HIPAA Electronic Transactions
- Answer your questions!!!

April 2007 - "Helping Frontline Users Perform Their

What is HIPAA?

Health Insurance Portability and Accountability Act

Enacted August 1996

Major Sections:

- Protect against job lock
- Standards for long term care insurance
- Major revisions to fraud and abuse provisions
- **Administrative Simplification**
  - ⇨ **Standardize the claim form**
  - ⇨ **Protect patient privacy/confidentiality**

Key Goals of HIPAA Administrative Simplification

Reduce paperwork

Improve efficiency of health systems

Protect security and confidentiality of electronic health information

Privacy v. Security

Privacy – *What* needs to be protected

- Protected Health Information (PHI)

Security – *How* will it be protected

- What if a breach occurs?

Privacy Standards – The Basics

A covered entity may not use or disclose protected health information unless the patient has authorized or consented, or unless HIPAA specifically permits or requires.

What is a covered entity:

- A health plan
- A health care clearinghouse
- A health care provider who transmits health information in electronic form
  - **UBO**

Privacy Standards – The Basics

If you are a covered entity, the rule applies for PHI in all forms (electronic, paper, verbal, etc. transactions).

Bottom line:

- Don’t use or disclose PHI unless:
  - Patient has consented or authorized, or
  - Regulation explicitly permits or requires.

This is why the DD Form 2569 is so important to the billing office!

Penalties for Violating Patient Privacy

Knowing disclosure of individually identifiable health information to another person:

- Up to $50,000, up to one year in prison or both

False pretenses

- up to $100,000, up to 5 years in prison, or both;

Intent to sell, transfer, use the information for commercial advantage, personal gain, or malicious harm

- up to $250,000, up to 10 years in prison, or both.

Uniformed Code of Military Justice (UCMJ), State or local regulations may apply

April 2007 – "Helping Frontline Users Perform Their

Notice of Privacy Practices (NOPP)

Should have been furnished to each existing patient by 14 April 2003 and made available to all new patients.

If there are any changes to the NOPP, it needs to be sent out again.

Patients should sign off on receiving the NOPP

Describes how a patient's PHI may be disclosed

- Treatment, Payment, Healthcare Operations
- Appointment reminders

NOTE: THESE ARE NOT UBO FUNCTIONS – INFORMATION ONLY

April 2007 – "Helping Frontline Users Perform Their

Notice of Privacy Practices (NOPP)

Disclosures permitted or required by law

- Public health
- Military/VA
- Law enforcement
- National Security
- Secretary of Health and Human Services (HHS)

NOTE: THESE ARE NOT UBO FUNCTIONS – INFORMATION ONLY

April 2007 – "Helping Frontline Users Perform Their

Notice of Privacy Practices (NOPP)

Patient's Rights

- Inspect and copy record
- Amend medical record (limited)
- Accounting of disclosures
- Request restrictions on access
- Submit a complaint
- Request confidential communications
- Receive a copy of the NOPP
- Designate a Personal Representative

NOTE: THESE ARE NOT UBO FUNCTIONS – INFORMATION ONLY

April 2007 – "Helping Frontline Users Perform Their

Authorization

Authorization allows use and disclosure of protected health information for purposes other than treatment, payment, and health care operations.

Must be written in specific terms.

Must include a start and end date or event.

May allow use and disclosure of protected health information by the covered entity seeking the authorization, or by a third party.

Treatment, Payment, Health Care Operations (TPO)

Treatment:

- The provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another

Payment:

- The various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care

April 2007 – "Helping Frontline Users Perform Their

Treatment, Payment, Health Care Operations (TPO)

Health Care Operations:

- Certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment

Individually Identifiable Health Information (IIHI)

Information about an individual that is:

- Created or received by a health care provider, health plan, employer, or health care clearinghouse; and
- Relates to:
  - the past, present, or future physical or mental health condition of an individual;
  - the provision of health care to an individual; or the past, present, or future payment for health care received by an individual; and that
- Either identifies the individual or provides a "reasonable basis" to believe the information can identify the individual.

Protected Health Information (PHI)

IIHI that is:

- Created or received by a covered entity
- Transmitted by electronic media;
- Maintained by electronic media;
- Transmitted or maintained in any other form or medium (including written or oral communications)

PHI excludes IIHI in:

- Education records covered by the Family Educational Rights and Privacy Act (FERPA)
- Employment records held by a CE in its role as an employer

April 2007, "Helping Frontline Users Perform Their

PHI Identifiers
(when attached to medical information)

- Names
- Geographic information (the first 3 digits of a zip code are allowed under limited circumstances)
- Dates (except year) directly related to an individual,
  - birth date,
  - admission date,
  - discharge date,
  - date of death;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social Security Numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers,
  -- including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Finger and voice prints;
- Full face photos

April 2007 - "Helping Frontline Users Perform Their

Minimum Necessary

- Requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for, PHI to the minimum necessary to accomplish the intended purpose
  - Limit information released to only what the person needs to know and release only the minimum amount of information
- Implementing the Requirement
  - Identify people or groups of people in the workforce who need access to PHI to do their work
  - Further identify the classes of PHI those individuals need to access

April 2007 – "Helping Frontline Users Perform Their

Minimum Necessary

Implementing the Requirement

- Create policies and procedures for **routine recurring** disclosures of PHI so that the information released is limited to the minimum to achieve the purpose of the disclosure
- Limit the PHI disclosed in **Non-routine** disclosures by developing criteria
- Review requests for PHI on an individual basis against the criteria

April 2007, "Helping Frontline Users Perform Their

Disclosures

DISCLOSURE	ACCOUNTING REQUIRED	ACCOUNTING **NOT** REQUIRED
*Covered entities **must** disclose PHI:*		
To the individual		X
To the Secretary of HHS for compliance investigation purposes	x	
*Covered entities **may** disclose PHI:*		
For treatment, payment, and healthcare operations (TPO) purposes		**X**
With authorization of the individual		X
Pursuant to a verbal agreement after individual has been given the opportunity to agree or object (e.g. facility directory, next of kin, close personal friend, person involved in individual's care) or for notification or emergency circumstance		x
Disclosures not permitted by law	X	
Without consent or authorization if:		
Incident to a permitted use or disclosure		X
Required by law if: related to child abuse, neglect, or domestic violence; in the course of judicial and administrative proceedings; or for law enforcement purposes	X	

April 2007 – "Helping Frontline Users Perform Their

Disclosures

DISCLOSURE	ACCOUNTING REQUIRED	ACCOUNTING **NOT** REQUIRED
*Covered entities **may** disclose PHI:*		
for certain public health activities including disclosures for the purpose of preventing or controlling disease and disclosures related to victims of child abuse or neglect	X	
Health Oversight	X	
About Decedents	X	
For Purposes of Cadaveric Organ Donation	X	
For Certain Research Purposes	X	
To Avert A Serious Threat to Health Or Safety	X	
For Specialized Government Functions	X	
For National Security or Intelligence Purposes		X
To Correctional Institutions	X	
For Worker's Compensation	X	
For Certain Marketing or Fundraising, Exceptions	X	
As Part of a Limited Data Set		X

April 2007 – "Helping Frontline Users Perform Their

De-Identified Health Information

- You may use PHI to create de-identified health information
- De-identified health information is not subject to regulation
- Two methods to verify de-identification of information:
  - Expert in statistical analysis and de-identification of information must analyze the information and attest that it does not contain elements that would identify an individual or aide in the identification of an individual when combined with other available data. The method of analysis and results must be documented
  - Remove the listed identifiers associated with the individual, relatives, employers or household members and any other information that might identify the individual

April 2007 – "Helping Frontline Users Perform Their

Security Breaches

What is a Breach?

- The unauthorized disclosure of information that compromises the security, confidentiality, or integrity of personally identifiable information (PII).

When can it occur?

- When unsecured PII is mishandled, lost or stolen or compromised.
- Hackers or insider threats.
- Inadvertent or malicious.

Source – Beyond the Basics: Proactive Strategy to Prevent Data Breaches, 2007 MHS Conference

April 2007 – "Helping Frontline Users Perform Their

Security Breaches

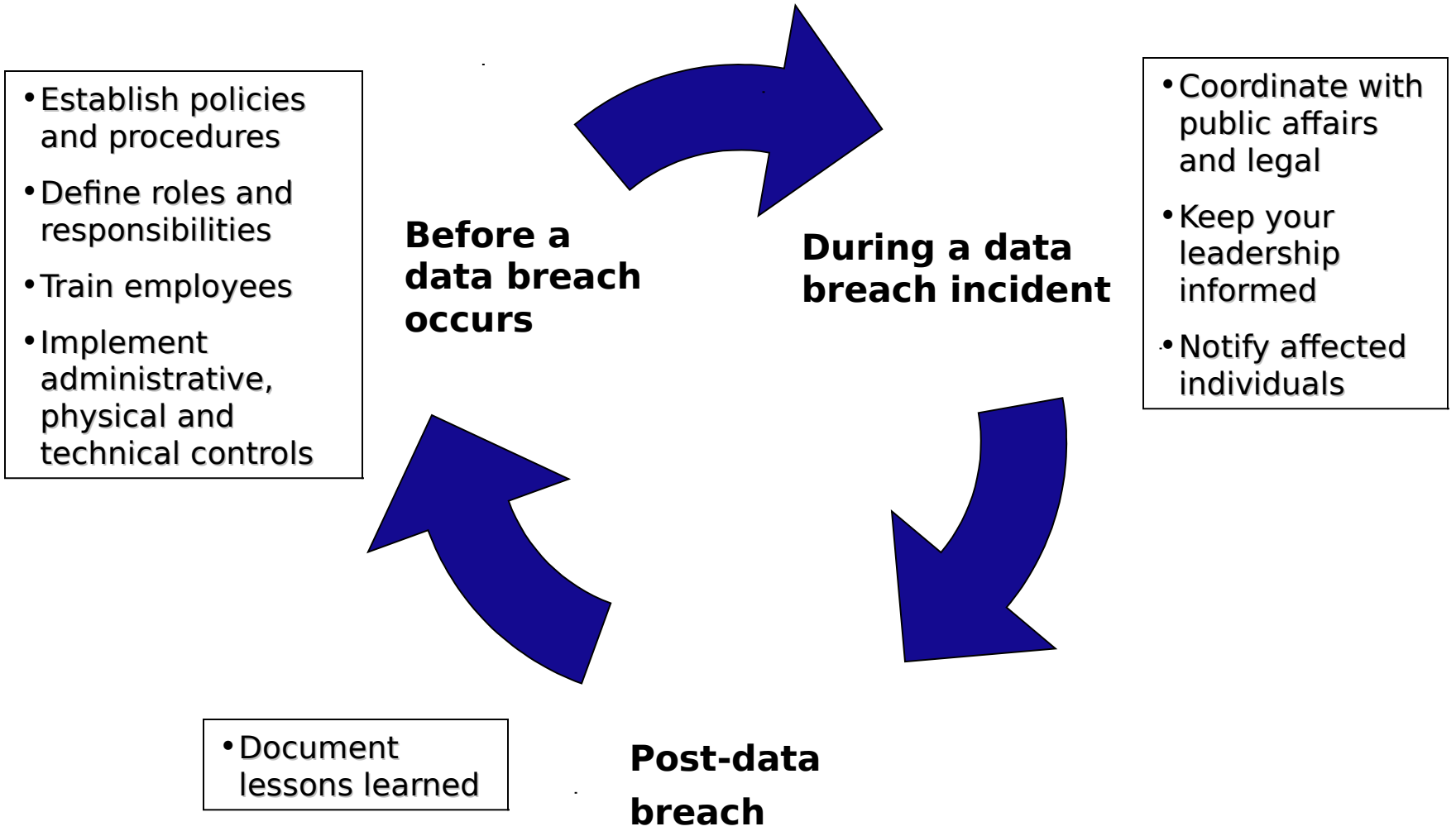
Occur in a variety of ways:

- Lost, stolen or misplaced computers, laptops, data storage (USB) devices, backup tapes, etc.;
- Information inappropriately transferred or sent out via e-mail; web mail, file transfer or instant messaging;
- Network data accessed by hackers or by employees without authorization;
- Hackers exploit viruses, Trojan Horses, or security loopholes to harvest information;
- Improper destruction of information – both physical (dumpsters) and electronic (PCs or laptops);
- Poor business practices or inadequate policy.

Source – Beyond the Basics: Proactive Strategy to Prevent Data Breaches, 2007 MHS Conference

April 2007 – "Helping Frontline Users Perform Their

Prevention Activities



Source – Beyond the Basics: Proactive Strategy to Prevent Data Breaches, 2007 MHS Conference

April 2007 – "Helping Frontline Users Perform Their

Avoiding Breaches

- Review your facility's information flow.
- Conduct periodic risk assessments.
- Identify where information resides.
- Train your employees on global policies *and* local procedures.
- Develop an Incident Response Plan.
- Don't install anything without the approval of your system administrator.
- Logoff when you leave your workstation.
- Don't open suspicious looking emails or attachments.

Source – Beyond the Basics: Proactive Strategy to Prevent Data Breaches, 2007 MHS Conference

April 2007 – "Helping Frontline Users Perform Their

Operationalizing HIPAA

- Identify who has access to PHI within your MTF
- Know your MTF's policies and procedures
  - How do you do things at your facility?
- If all else fails, call your MTF's Privacy Officer

April 2007 – "Helping Frontline Users Perform Their

Operationalizing HIPAA

- Things to consider
  - Computer accessibility
  - Talking in the halls
  - Discipline for privacy violations
  - Limit information sent or forwarded in emails

April 2007 – "Helping Frontline Users Perform Their

Transaction Standards

- What are transactions?
  - Activities involving the transfer of health care information for specific purposes.

- HIPAA requires
  - Providers engaging certain transactions to comply with the standard for the particular transaction.
  - Providers doing business electronically to use the same health care transactions, code sets, and identifiers.

Transaction Standards

- Standard transactions for Electronic Data Interchange (EDI) to transmit health care data include:
  - Claims and encounter information,
  - payment and remittance advice, and
  - claims status and inquiry

- Code sets
  - Codes used to identify specific diagnosis and clinical procedures on claims and encounter forms.
    - Examples: HCPCS, CPT-4, ICD-9, NDCs

Transaction Standards

- Claims or Encounters
  - 837P: Paper CMS 1500
  - 837I: Paper UB-04
- 835: Payment/Remittance Advice (EOB)
- 270: Eligibility Benefit Inquiry
- 271: Eligibility Benefit Response
- 278: Health Care Services Review (request for review and response – precerts/referral authorizations)
- 276: Health Care Claim Status Request
- 277: Health Care Claim Status Response

Resources

Legislation

- HIPAA: P.L. 104-191 (HR 3103), August 21, 1996
- ASCA: P.L. 107-105 (HR 323), December 2001

Regulation

- 45 CFR SUBCHAPTER C--ADMINISTRATIVE DATA STANDARDS AND RELATED REQUIREMENTS (Parts 160, 162, 164)

TMA

- http://www.tricare.mil/hipaa/
- http://www.tricare.mil/tmaprivacy/

Resources

- DoDD 6025.18 - *Privacy of Individually Identifiable Health Information in DoD Health Care Programs*
- DoD 6025.18-R - *DoD Health Information Privacy Regulation*
- HA Policy 06-010 - HIPAA Security Compliance

Summary

- Review those parts of the Health Insurance Portability and Accountability Act that apply to UBO staff
  - Privacy
    - A brief history, what is PHI, what can the billing office disclose
  - Security
    - How can a security breach occur
    - How to avoid a breach
  - HIPAA Electronic Transactions
- Answer your questions!!!

Questions?

UBO Help Desk

ubo.helpdesk@altarum.org

703-575-5385

Teleconference Evaluation

Was this teleconference helpful?

Please send comments/suggestions to

UBO.Helpdesk@Altarum.org

Have we missed a topic?

Please send suggestions for future teleconferences to

UBO.Helpdesk@Altarum.org